



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/695,277	10/28/2003	Yong Ho Son	007412.00304	3963
71867 7590 11/24/2009 BANNER & WITCOFF, LTD ATTORNEYS FOR CLIENT NUMBER 007412 1100 13th STREET, N.W. SUITE 1200 WASHINGTON, DC 20005-4051			EXAMINER SAINT CYR, JEAN D	
			ART UNIT 2425	PAPER NUMBER
			MAIL DATE 11/24/2009	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/695,277

**Applicant(s)**

SON ET AL.

**Examiner**

JEAN D. SAINT CYR

**Art Unit**

2425

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 July 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 2-10 and 12-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 2-10 and 12-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB-06)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

**Response to Amendment**

This action is in response to applicant's amendment filed 07/24/2009. claims 1 and 11 were cancelled. Claims 12-20 were added. **This action is made FINAL.**

**Response to arguments**

Applicant's arguments with respect to claims 2-10, 12-20 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-10, 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Redmond et al in view of Heer et al, US No.5999629.

Re claim 2, Redmond et al disclose wherein the remote server is adapted to cause transmission of a decryption key to said-the requesting subscriber the decryption key being necessary to decrypt the video program(On the user's side, the decryption key is used to decrypt the media file, col.12, lines 30-31).

Re claim 3, Redmond et al did not explicitly disclose the video program in the second encrypted form is encrypted according to a public key associated with the requesting subscriber, the public key having an associated with it a private key necessary to decrypt the video program in the second encrypted form.

However, Heer et al disclose the video program in the second encrypted form is encrypted according to a public key associated with the requesting subscriber, the public key having an associated with it a private key necessary to decrypt the video program in the second encrypted form(public key generated by a security module associated with the requester,col.2, lines 1-2;private key, col.4, line 34; decrypt the encrypted program, col.4, line 7).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to incorporate the teaching of Heer into the invention of Redmond for the purpose of making the system safer against unauthorized user in using private key and public key before decrypting a program.

As claim 4, the claimed "the private key having an associated public key necessary to decrypt the video program in the second encrypted form..." is composed as the same structural elements as previously discussed with respect to claim 3.

Re claim 5, Redmond et al did not explicitly disclose wherein the video program in the second encrypted form is encrypted according to a public key, the public key having an associated private key necessary to decrypt the video program in the second encrypted form, the system further comprising: the remote server transmitting the private key to the requesting subscriber.

However, Heer et al disclose wherein the video program in the second encrypted form is encrypted according to a public key, the public key having an associated private key necessary to decrypt the video program in the second encrypted form, the system further comprising: the remote server transmitting the private key to the requesting subscriber(see fig.1, element 60; server 60 then transmits the message in sequence with other such messages to communications path 61 for transmission to the subscriber terminals, col.7, lines 45-48).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to incorporate the teaching of Heer into the invention of Redmond for the purpose of allowing only authorized requested users to decrypt the content.

Re claim 6, Redmond et al did not explicitly disclose the private key is encrypted prior to transmission to the requesting subscriber.

However, Heer et al disclose the private key is encrypted prior to transmission to the requesting subscriber(The private key is another device unique encryption key, S.sub.id, that is also generated during the manufacture of the respective module and stored in a secured/protected memory location, col.4, lines 34-38).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to incorporate the teaching of Heer into the invention of Redmond for the purpose of allowing the terminal to receive the private key before any request.

Re claim 7, Redmond et al did not explicitly disclose wherein the remote is adapted to transmit the video program in the second encrypted form to the requesting subscriber via a first communications channel and is adapted to transmit a decryption key to the requesting subscriber via a second communications channel.

However, Heer et al disclose wherein the remote is adapted to transmit the video program in the second encrypted form to the requesting subscriber via a first communications channel and is adapted to transmit a decryption key to the requesting subscriber via a second communications channel(see fig.1, the system uses bus 41 for encrypted video program and bus 61 for sharing key; col.6, lines 17-24).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to incorporate the teaching of Heer into the invention of Redmond

for the purpose of allowing the system to use two different channels for transmitting keys and video.

Re claim 8, Redmond et al disclose wherein the video program in the second encrypted is encrypted according to a Data Encryption Standard "DES"( provides digital protection of the media file by encrypting it using strong encryption algorithms 46 such as CAST-128, IDEA, Triple-DES, or other high-grade encryption technology,col.6,lines 29-32).

Re claim 9, Redmond et al disclose did not explicitly wherein the remote server is adapted to multiplex the video program in the second encrypted form and other signals to create a multiplexed signal for transmission to the requesting subscriber.

However, Heer et al disclose wherein the remote server is adapted to multiplex the video program in the second encrypted form and other signals to create a multiplexed signal for transmission to the requesting subscriber(multiplexer, col.9. lines 63-65).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to incorporate the teaching of Heer into the invention of Redmond for the purpose of allowing the system to transmit a plurality of signals in one channel.

Re claim 10, Redmond et al disclose further comprising the at least one programming source wherein the at least one programming source comprises at least one of a television broadcasting source, a premium broadcast source, and a video-on-demand source (see fig.1; video-on-demand systems, col.4, lines 32).

Re claim 12, Redmond et al disclose an interactive information distribution system comprising: a distribution center comprising a remote server(see fig.3);

the remote server configured to store in storage a video program encrypted in a

first encrypted form received from at least one programming source which is located remote from the remote server(see fig.3, element 26; The resulting media file archive 26, which has been optionally compressed, watermarked, and encrypted, is stored in the media file database 18,col.6, lines 34-36; the preferred system of the present invention incorporates pre-encrypted media file data stored in the media file database,col.4, lines 47-49)

the remote server configured to retrieve the video program encrypted in the first encrypted form from the storage and processing the video program encrypted in the first encrypted form responsive to a subscriber request to produce a decrypted video program(media file archive comprising one or more pre-compressed and pre-encrypted media data files, said server being for receiving one or more transmission requests for a selected media file from a plurality of users,col.2, lines 34-38).

But did not explicitly disclose the remote server configured to process the decrypted video program to produce a video program in a second encrypted form; and the remote server configured to transmit the video program in the second encrypted form to the requesting subscriber.

However, Heer et al disclose the remote server configured to process the decrypted video program to produce a video program in a second encrypted form; and the remote server configured to transmit the video program in the second encrypted form to the requesting subscriber(decrypts the encrypted program encryption key using CV. Module 50 then re-encrypts the program encryption key using its device unique key, col.5, lines 59-62; Processor then transmits the message over bus 41 for distribution to the subscriber terminals, col.7, lines 17-18).

It would have been obvious for any person of ordinary skill in the art at that time the invention was made to incorporate the teaching of Heer into the invention of Redmond

for the purpose of making the system safer against unauthorized user in using re-encryption or double encryption technique.

As claim 13, the claimed "the remote server configured to process a video program encrypted in the first encrypted form received from at least one programming source, which is located remote from the remote server, to produce a decrypted video program..." is composed as the same structural elements as previously discussed with respect to the rejection of claim 12.

Re claim 14, is met as previously discussed with respect to claim 2.

Re claim 15, is met as previously discussed with respect to claim 5.

Re claim 16, is met as previously discussed with respect to claim 6.

Re claim 17, is met as previously discussed with respect to claim 7.

Re claim 18, is met as previously discussed with respect to claim 8.

Re claim 19, is met as previously discussed with respect to claim 9.

Re claim 20, is met as previously discussed with respect to claim 10.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jean Duclos Saintcy whose phone number is 571-270-3224. The examiner can normally reach on M-F 7:30-5:00 PM EST. If attempts to reach the examiner by telephone are not successful, his supervisor, Brian Pendleton, can be reached on 571-272-7527. The fax number for the organization where the application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Retrieval (PAIR) system. Status information for published applications may be obtained from either private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the



Art Unit: 2425

automated information system, dial 800-786-9199(IN USA OR CANADA) or 571-272-1000.

/Jean Duclos Saintcyr /

/Brian T. Pendleton/

Supervisory Patent Examiner, Art Unit 2425